Good morning Mr. Chairman and distinguished guests. The tremendous advances being made in the computer and telecommunications industries are forever changing the way we do business in this country and abroad. This new digital age in which we are living has ushered in the ability to trade stock, shop for a car, buy air line tickets and to buy, sell and trade just about anything else using the Internet. Many of the firms that are engaging in this new way of doing business didn=t exist a few years or even months ago. The growth of e-commerce has been so rapid that projections made about how much business will be conducted over the Internet were often outdated as soon as they are published. On March second of this year the Commerce Department released the first ever estimate of retail e-commerce sales or e-tail sales. Reported e-tail sales over the Internet and other electronic networks have reached a historic $5.3 billion in the fourth quarter of 1999.

While there are now new opportunities for the good people of our nation to gain greater productivity and have access to a wider selection of goods and services, there is an attendant menace to on-line businesses which threatens to disrupt the way commerce is conduced over the Internet. This menace is **HACKERs** who are seeking to gain unauthorized access to systems for the purpose of destroying, corrupting, stealing or monitoring information vital to the operation of computer systems owned by others.

These hackers have distinguishing screen names, or aliases, and are apparently very bright, intelligent people with deviant, malicious minds and a hankering for chaos. One suspected hacker is a 17 year-old New England boy who told investigators that he has been using computers since he was three and spends 16 hours a day on the Internet.

All businesses must be protected from the hackers, but no where is it more important than the businesses and industries that are vital to the nation=s health, wealth and security and make up our nation=s critical infrastructure. These critical infrastructure businesses and industries are engaged in information and communications, banking and finance, basic utilities, aviation, mass transit, public health services, and oil and gas production and storage. On the Government side, the critical infrastructure consists of internal security, federal law enforcement, foreign intelligence, foreign affairs and national defense. All of these activities must be protected from the destructive, corruptive, stealing or monitoring of information by unauthorized persons. Anyone attempting to hack into these systems must be stopped because their actions threaten our country=s security.

A GAO report released March second of this year provides commentary on the proposed Government Information Security Act and cites some very disturbing facts about the state of the Government=s computer security:

The Environmental Protection Agency has had invasions of its systems that resulted in damage and disruption to that agency=s operations.

The Department of Veterans Administration has been cited for weaknesses in its computer systems that could compromise sensitive medical and benefit payment information of our nation=s veterans.

A test on the National Aeronautics and Space Administration=s systems reveled that their systems could have been penetrated posing serious threats to orbiting spacecraft and the scientific data received from these spacecraft.

The State Department=s computers are also vulnerable to attack and unauthorized access by hackers, terrorists or other unauthorized individuals.

It appears that from this listing that there is a pressing need to improve computer security planning and management and to make the cases like these just cited the exception, not the rule in the government=s systems.

Fear, mistrust and the uncertainties created by hackers can slow the economic growth and prosperity that many public and private sector experts envision for the Internet. As the Government sets out to continue to protect our nation=s critical infrastructure from domestic and foreign intruders and e-businesses set out to reduce the costs of theft and destruction of data and hardware by hackers, we must ensure that people seeking to do business over the Internet are safe from hackers, and that sufficient cooperation and coordination between the government and private industry is encouraged. Most recently this cooperation resulted in a smooth transition to the year 2000. We can and must replicate these results in the area of computer security.

I am very interested in hearing from the panel about your thoughts with regard to the scope and magnitude of the hacker problem and what your recommendations are for putting hackers out of business.